IN THE CLAIMS:

1. (Original) A method of encryption, comprising:

(a) partitioning an input message into matrix elements;

(b) computing the determinant of said matrix;

(c) encrypting said determinant; and

(d) multiplying said matrix by said encrypted determinant.

2. (Original) The method of claim 1, further comprising:

(a) prior to step (a) of claim 1, preprocessing said input message wherein said preprocessing includes a permutation of the message.

3. (Original) The method of claim 1, wherein:

(a) said permutation of step (a) of claim 2 is generated by a hash of said input message.

4. (Original) The method of claim 1, wherein:

(a) said permutation of step (a) of claim 2 is generated by a random sequence.

5. (Original) The method of claim 2, wherein:

(a) said preprocessing of step (a) of claim 2 includes exclusive ORing said message after permutation with generators of said permutation.

6. (Original) The method of claim 1, wherein:

(a) said encrypting of step (c) of claim 1 is public-key encryption.

7. (Original) The method of claim 6, wherein:

(a) said public-key encryption is RSA.

8. (Original) The method of claim 1, wherein:

(a) said partitioning of step (a) of claim 1 first fills the principal diagonal of said matrix.

9. (Currently Amended) A method of encryption, comprising:

(a) defining a permutation source; ~~preprocessing an input message wherein said preprocessing includes a permutation of the message; and~~

(b) generating a permuted message for an input message employing said permutation source;

(c) padding said permuted message with said permutation source to obtain a preprocessed message; and

(d) encrypting said preprocessed message with block-based encryption method which has blocks smaller than said preprocessed message.

10. (Currently Amended) The method of claim 9, wherein:

~~(a)~~ said permutation source ~~of step (a) of claim 9~~ is generated by a hash of said input message.

11. (Currently Amended) The method of claim 9, wherein:

~~(a)~~ said permutation source ~~of step (a) of claim 9~~ is generated by a random sequence.

12. (Currently Amended) The method of claim 9, wherein:

~~(a)~~ said block-based encryption ~~of step (b) of claim 9~~ is a public key encryption.

13. (Original) A method of decrypting, comprising:

(a) computing the determinant of a matrix-based encrypted message matrix;

(b) decrypting said determinant; and

(c) multiplying said matrix by the results of step (b).

14. (Original) The method of claim 13, wherein:

(a) when said matrix-based encrypted message of step (a) of claim 13 had preprocessing

including a permutation, applying the inverse of said permutation to the results of step (c) of claim 13.

15. (New) The method of claim 9, wherein said padding includes prepending said permuted message with said permutation source to obtain said preprocessed message.

16. (New) The method of claim 9, wherein said padding includes appending said permuted message with said permutation source to obtain said preprocessed message.